

**QUICK RESPONSE PASSWORD PADA AUTENTIKASI BARANG
MENGUNAKAN ALGORITMA AES**

SKRIPSI

Diajukan untuk Memenuhi Salah Satu Syarat Mencapai Gelar Strata Satu

Jurusan Informatika



Disusun oleh :

Ashar Wirawan

NIM. M0510012

**JURUSAN INFORMATIKA
FAKULTAS MATEMATIKA & ILMU PENGETAHUAN ALAM
UNIVERSITAS SEBELAS MARET
SURAKARTA
2014**

commit to user

SKRIPSI

**QUICK RESPONSE PASSWORD PADA AUTENTIKASI BARANG
MENGUNAKAN ALGORITMA AES**

Disusun oleh :
Ashar Wirawan
M0510012

**Skripsi ini telah disetujui untuk dipertahankan di hadapan dewan
penguji pada tanggal 16 September 2014**

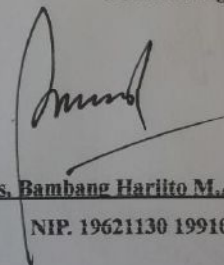
Skripsi ini telah disetujui untuk dipertahankan di hadapan dewan
penguji pada tanggal 16 September 2014

Pembimbing I,



Esti Survani, S.Si., M.Kom.
NIP. 19761129 200812 2 001

Pembimbing II,




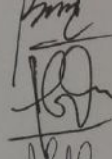
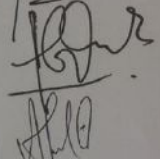

Drs. Bambang Hariyanto M.App.Sc.Ph.D.
NIP. 19621130 199103 1 002

SKRIPSI
QUICK RESPONSE PASSWORD PADA AUTENTIKASI BARANG
MENGGUNAKAN ALGORITMA AES

Disusun oleh :
Ashar Wirawan
M0510012

Telah dipertahankan di hadapan Dewan Penguji
Pada tanggal : 16 September 2014

Susunan Dewan Penguji

- | | | | |
|---|---|--|---|
| 1. <u>Esti Suryani, S.Si., M.Kom.</u> | (|  |) |
| NIP. 19761129 200812 2 001 | | | |
| 2. <u>Drs. Bambang Harjito M.App.Sc.Ph.D.</u> | (|  |) |
| NIP. 19621130 199103 1 002 | | | |
| 3. <u>Abdul Aziz, S.Kom., M.Cs.</u> | (|  |) |
| NIP. 19810413 200501 1 001 | | | |
| 4. <u>Afrizal Doewes S.Kom., M.Sc.</u> | (|  |) |
| NIP. 19850831 201212 1 004 | | | |

Disahkan oleh:


Prof. Ir. Ari Handono Ramelan, M.Sc. (Hons), Ph.D.
NIP. 19610223 198601 1 001

Ketua Jurusan Informatika

Drs. Bambang Harjito M. App.Sc.Ph.D.
NIP. 19621130 199103 1 002

MOTTO

Be a blessing for everything around you

(Penulis)

You only live once, but if you do it right, once is enough

(Mae West)



PERSEMBAHAN

Karya ini Penulis persembahkan kepada:

“Ayah, Ibu, Adik, dan seluruh keluarga besar.”

“Teman-teman Informatika 2010 khususnya Hedik, Cerren, Adit, Taufik, Viko, April, Lydia, Aji, Miftah, Dian”



KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan kesempatan kepada penulis untuk menyelesaikan Tugas Akhir ini. Pada Tugas Akhir ini, penulis menerapkan algoritma *Advanced Encryption Standard* dan *Quick Response Code* dalam Kasus Autentikasi Barang. Penulis menyadari akan keterbatasan yang dimiliki. Begitu banyak bantuan diberikan dalam penyusunan Tugas Akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Ir. Ari Handono Ramelan, M.Sc. (Hons), Ph.D selaku Pimpinan Fakultas MIPA Universitas Sebelas Maret Surakarta,
2. Bapak Drs. Bambang Harjito M.App.Sc,Ph.D. selaku Ketua Jurusan Informatika FMIPA UNS sekaligus sebagai Dosen Pembimbing II yang telah memberikan masukan, kritik dan saran yang membangun,
3. Ibu Esti Suryani, S.Si., M.Kom. Selaku Dosen Pembimbing I yang telah memberikan pengarahan selama proses penyusunan Tugas Akhir ini,
4. Bapak *Abdul Aziz*, S.Kom, M.Cs. selaku anggota penguji yang telah memberikan masukan, kritik dan saran yang membangun,
5. Bapak Afrizal Doewes S.Kom, M.Sc. selaku anggota penguji yang telah memberikan masukan, kritik dan saran yang membangun,
6. Ayah, ibu, dan adik-adikku yang senantiasa memberikan dukungan dan motivasi,
7. Teman-teman yang senantiasa selalu berbagi pengetahuan, pengalaman, dan memberikan dukungan dan motivasi.

Semoga Tugas Akhir ini bermanfaat bagi semua pihak yang berkepentingan.

Penulis

QUICK RESPONSE PASSWORD FOR GOODS AUTHENTICATION USING AES ALGORITHM

Ashar Wirawan

Jurusan Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam.

Universitas Sebelas Maret

ABSTRACT

Nowadays the authentication process of goods shipping company uses a shipment receipt and an ID card. The problem is that courier does not use the right procedure of the goods revenue. As a result, it causes the wrong receiver. Based on this problem, a study will be conducted to represent the goods authentication process through a Quick Response Password system. It uses a QR Code scanning procedure to prove that the goods was accepted by the receiver.

Advanced Encryption Standard (AES) is used in this thesis to encrypt the ID transaction. It was chosen due to the short time of encryption and decryption. QR Code was chosen over another 2 dimension barcode because of the high endurance of QR Code, the easy scanning process by mobile phone camera and it is open source. QR Code was implemented as a package in the distribution of ciphertext. Packaging data by QR Code was expected to simplify the authentication process by scanning.

The result shows that the ID transaction of goods were successfully encrypted and generated a QR Code. It will be used in the goods authentication process. QR Code indicates robustness to physical damage. The damage percentage limit which still can be recovered for unite and spread blocking were 21% and 12%, then for the distorting was 30%.

Keywords : QR Code, Authentication, *Advanced Encryption Standard*

QUICK RESPONSE PASSWORD PADA AUTENTIKASI BARANG MENGUNAKAN ALGORITMA AES

Ashar Wirawan

Jurusan Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam.

Universitas Sebelas Maret

ABSTRAK

Proses autentikasi barang pada jasa pengiriman barang saat ini menggunakan kertas bukti resi barang dan Kartu Tanda Penduduk (KTP). Permasalahan yang muncul adalah kurir tidak selalu melakukan prosedur penerimaan barang dengan benar. Hal itu menimbulkan terjadinya kesalahan penerima barang. Berdasarkan hal tersebut, dilakukan penelitian yang bertujuan untuk merepresentasikan proses autentikasi barang melalui suatu sistem *Quick Response Password*. Sistem mengharuskan prosedur *scanning QR Code* dilakukan sebagai bukti barang telah sampai pada penerima.

Advanced Encryption Standard (AES) dalam penelitian ini digunakan untuk mengenkripsi ID transaksi. *AES* dipilih karena memiliki waktu enkripsi dan dekripsi yang relatif lebih cepat. *QR Code* dipilih dari beberapa jenis barcode 2 dimensi karena memiliki ketahanan yang cukup tinggi, proses *scanning* yang hanya menggunakan kamera *mobile phone* dan dapat digunakan dengan gratis. *QR Code* diimplementasikan sebagai *package* dalam pendistribusian *ciphertext*. Penggunaan *QR Code* diharapkan dapat mempermudah proses autentikasi melalui cara *scanning*.

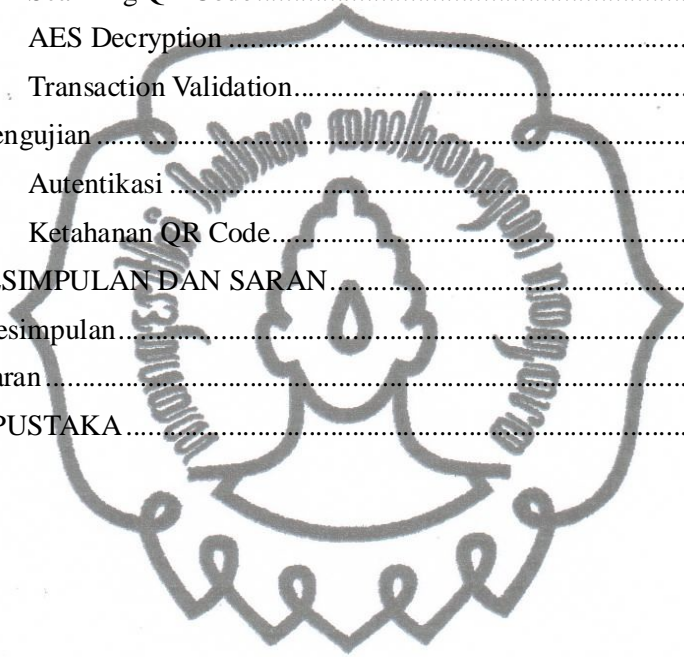
Hasil pengujian menunjukkan bahwa ID transaksi berhasil dienkripsi dan digenerate menjadi *QR Code*. Hasil *QR Code* kemudian digunakan dalam proses autentikasi barang. Uji ketahanan *QR Code* menunjukkan bahwa persentasi batas kerusakan yang masih dapat dikoreksi untuk uji *blocking* menyatu dan menyebar sebesar 21% dan 12%, sedangkan untuk uji *distorsing* sebesar 30%.

Kata Kunci : *QR Code*, Autentikasi, *Advanced Encryption Standard*

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	ii
MOTTO.....	iii
PERSEMBAHAN.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	2
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	3
BAB II LANDASAN TEORI.....	5
2.1 Landasan Teori.....	5
2.1.1 Kriptografi.....	5
2.1.2 QR Code.....	6
2.1.3 <i>Advanced Encryption Standard (AES)</i>	10
2.2 Penelitian Terkait.....	16
BAB III METODOLOGI PENELITIAN.....	19
3.1 Perancangan Alur Sistem.....	19
3.2 Prosedur Pengujian.....	22
3.3 Implementasi.....	23
BAB IV HASIL DAN PEMBAHASAN.....	24

4.1	Pembahasan	24
4.1.1	Data Validation.....	24
4.1.2	AES Encryption	24
4.1.3	Generate QR Code	33
4.1.4	Scanning QR Code.....	43
4.1.5	AES Decryption	43
4.1.6	Transaction Validation.....	44
4.2	Pengujian	45
4.2.1	Autentikasi	45
4.2.2	Ketahanan QR Code.....	46
BAB V KESIMPULAN DAN SARAN.....		50
5.1	Kesimpulan.....	50
5.2	Saran.....	50
DAFTAR PUSTAKA.....		51



DAFTAR TABEL

Tabel 2.1 Spesifikasi QR Code	9
Tabel 2.2 Jenis AES.....	11
Tabel 2.3 Kelebihan dan Kekurangan Penelitian Terkait	17
Tabel 2.4 Matrik Keterkaitan Penelitian Terkait dengan Penelitian ini	18
Tabel 4.1 Heksadesimal Kunci.....	25
Tabel 4.2 Hasil Rot Word	25
Tabel 4.3 Hasil Sub Word.....	26
Tabel 4.4 Rcon	26
Tabel 4.5 Proses Lanjutan Rcon.....	27
Tabel 4.6 Kunci Round 0 - 8	27
Tabel 4.7 Kunci Round 9 - 15	28
Tabel 4.8 Plaintext.....	28
Tabel 4.9 Hasil XOR Plaintext dan Kunci	29
Tabel 4.10 Hasil Sub Byte.....	29
Tabel 4.11 Hasil Shift Row	29
Tabel 4.12 Proses Mix Column.....	30
Tabel 4.13 Proses Mix Column.....	31
Tabel 4.14 Matriks Hasil Mix Column	32
Tabel 4.15 Hasil Padding QR Code	33
Tabel 4.16 Susunan Codeword.....	35
Tabel 4.17 Mask Pattern.....	39
Tabel 4.18 Bit Identitas QR Code	41
Tabel 4.19 Matriks Multiplikasi AES Dekripsi.....	44
Tabel 4.20 Hasil Pengujian Autentikasi	45
Tabel 4.21 Hasil Uji Coba Blocking Menyatu	46
Tabel 4.22 Hasil Uji Coba Blocking Menyebar	47
Tabel 4.23 Hasil Uji Coba Distorsing	48
Tabel 4.24 Batas Maksimal Recovery Setiap Level.....	49

DAFTAR GAMBAR

Gambar 2.1 Diagram Kriptografi Berdasar Jenis Kunci	5
Gambar 2.2 Struktur QR Code	6
Gambar 2.3 Koreksi Distorsing Simbol	8
Gambar 2.4 Detail Proses Key Schedule 1	12
Gambar 2.5 Proses Key Schedule 2	12
Gambar 2.6 Proses Key Schedule 3	13
Gambar 2.7 Proses Key Schedule 4	13
Gambar 2.8 S-Box	13
Gambar 2.9 Proses Sub Bytes	14
Gambar 2.10 Proses Shift Rows	14
Gambar 2.11 Proses MixColumn	15
Gambar 2.12 Proses Add Round Key	15
Gambar 3.1 Bagan Utama Sistem Autentikasi	19
Gambar 3.2 Alur Proses Encode dan Decode dari Sistem Autentikasi	20
Gambar 3.3 Proses Enkripsi AES	21
Gambar 3.4 Proses Dekripsi AES	22
Gambar 4.1 L Galois Field	30
Gambar 4.2 E Galois Field	31
Gambar 4.3 Polinomial Data Codeword	36
Gambar 4.4 Generator Polinomial	36
Gambar 4.5 Polinomial Hasil	37
Gambar 4.6 Penambahan Data Bit ke Atas	38
Gambar 4.7 Penambahan Data Bit ke Bawah	38
Gambar 4.8 Total Pinalti QR Code Hasil Masking	40
Gambar 4.9 Posisi Data Bit Error Correction dan Mask Pattern	41
Gambar 4.10 Posisi Data Bit Versi QR Code	42
Gambar 4.11 Hasil QR Code	42
Gambar 4.12 S-Box Inverse	44

DAFTAR LAMPIRAN

Form Pengiriman Barang	52
Halaman Form Password	53
Report Autentikasi Sukses	53

